Description

Method and device for authenticating a subscriber for utilizing services in a wireless LAN (WLAN) while using an IP multimedia subsystem (IMS) of a mobile radio network.

The invention relates to a method and device for authenticating a subscriber for utilizing services in a wireless LAN (WLAN) while using an IP multimedia subsystem (IMS) of a mobile radio network.

A method for authenticating WLAN subscribers in a mobile radio network is known from the journal "Funkschau", issue 09/2002, pages 14-15, namely authentication via a NAI (Network Access Identifier) and optionally via a SIM card, and authentication using the IPv6 (Internet Protocol Version 6) and a so-called SIM-6 mechanism. In general, authentication of a wireless LAN subscriber is effected via an HTTP protocol.

WO 00/76249 A1 describes a method of authorizing an Internet protocol-enabled mobile device to access the Internet via a wireless LAN (WLAN), GSM or UMTS network, whereby the transmission of an IP access request is initiated from the mobile device to an IP router via the access network. In response to receipt of said access request at the IP router, an IP address routing prefix is sent from the IP router to the mobile device. The IP router then only forwards IP packets to the mobile device if it has first received an authorization message from a control point. The control point monitors the payment (electronic cash) from the mobile device for use of the Internet.

US 2002/0062379 A1 describes the setting up of a multimedia session involving a mobile device with a session packet access bearer, which is established between the mobile device and an access point to a packet data network via a radio access network. The access point is connected to a multimedia system that supports multimedia session services. Using the session packet access bearer, a multimedia session that includes a plurality of media data streams is initiated in a mobile device. Media packet access bearers are established between the mobile device and the access point.

The object of this invention is to efficiently authenticate a subscriber of a wireless LAN who is also a mobile radio network subscriber, while utilizing services in a mobile radio network.

The object is achieved according to the invention by the objects of the independent claims with reference to the method and device. Developments of the invention are specified in the subclaims. Authentication while using an IP multimedia subsystem, according to the invention, has the advantage that a subscriber is authenticated for any services that can be reached via the wireless LAN, without the installation of a separate server for authentication in the wireless LAN and without separate connection to a corresponding entity in the mobile radio network (e.g. HLR/HSS), which must be contacted by means of a connection (interface) especially provided for that purpose.

The invention is explained in greater detail with the help of an exemplary embodiment illustrated in the diagrams. In particular,

Figure 1 shows the architecture with the interfaces between a wireless LAN and an IP multimedia subsystem (IMS)

Figure 2 shows how the WAGW obtains the authentication result using a separate P-CSCF/policy control function at the location having WLAN coverage

Figure 3 shows how the WAGW obtains the authentication result through the P-CSCF/policy control function of the IP multimedia subsystem (IMS)

Figure 4 shows how the WAGW learns the authentication result by expanded functionalities

Figure 1 shows how the wireless LAN is connected to an IP multimedia subsystem (IMS) (3). A subscriber MT (6) of a wireless LAN (10) is connected via a radio interface (11) to the wireless LAN at a location having wireless LAN coverage (hotspot). For the authentication, the subscriber MT (6) receives an IP address (e.g. through DHCP) from the proxy call state control function node (P-CSCF)(1). The subscriber MT (6) can thus authenticate himself, by means of SIP registration, in the IMS (3) without any prior bearer level authentication (e.g. H/2, authentication via the radio interface is optional). In the IMS (3), the authentication takes place on the application side in the call state control function node (CSCF) (4) via an SIP registration message. This authentication guarantees the MT (6) access to specific profiles (e.g. WLAN profiles). The CSCF (4) uses an authentication that is known per se for the IMS (3), but not for a WLAN (10), by means of the home subscriber system (HSS) (5) via the Cx interface. The P-CSCF (1) of the WLAN (10) receives the result of the authentication via an SIP registration request (e.g. 200 OK). This result is transferred to the WLAN access gateway (WAGW) (2). The WAGW (2) controls the access to services and monitors the successful authentication in the IMS (3). The wireless LAN (10) is connected to the Gi interface or Mm interface with the IMS (3). The Gi interface is an interface within the IP network (7) and is thus subject to special security precautions. The geographical distance between the IMS (3) and the location having WLAN coverage is also taken into account. At the Mm interface, the connection between the IMS (3) and the location having WLAN coverage (hotspot) is effected via an IP multimedia network (Internet) (8).

The authentication of an MT (6) in the IMS (3) is carried out using the SIP protocol. The result of the authentication in the IMS (3) is fed to the WAGW (2). There are three options for this, which are described under Figure 2, Figure 3 and Figure 4.

Figure 2 shows how the WAGW (2) receives the authentication result through a separate P-CSCF (1)/policy control function at the location having WLAN coverage (hotspot). In this case the WLAN (10) is equipped with its own P-CSCF (1), which is used for forwarding SIP messages to the corresponding entity in the IMS (3) (SIP registration request) and controlling the WAGW (2) according to the authentication result of the IP multimedia subsystem (IMS) (SIP response). The P-CSCF (1) communicates with the CSCF (4) in the IP multimedia subsystem via a Gi interface or Mm interface (via Internet (8)). The P-CSCF (1) provides the WAGW (2), on the basis of the result of the authentication (SIP registration) in the IMS (3), with instructions on how the data traffic of an MT (6) is to be handled by the WAGW (2). This enables the WAGW (2) to block the data flow, for example. By means of the policy control function, the P-CSCF(1) controls the data traffic through the WAGW (2), and is able to grant, restrict, increase or decline the quantity and quality of the data flow of an MT (6) through the WAGW (2). This mechanism is similar to the Go interface which is installed between the P-CSCF of the IMS (3) and the gateway GPRS support node (GGSN) (9). This policy control function may be part of the P-CSCF(1) or may even be a separate unit, which may optionally be used in addition for the IP multimedia subsystem and the PS domains.

One possible policy protocol is COPS (RFC 2748, used for the Go interface). The Go interface uses an IP transport, and therefore a protected transfer of COPS messages within the wireless LAN, or a separate connection (i.e. separated from data traffic of subscribers within the wireless LAN) between P-CSCF(1) and WAGW (2,) is installed during implementation.

Figure 3 shows how the WAGW (2) is notified of the result of the IMS authentication by the CSCF (4) of the IMS (3). The CSCF (4) of the IMS (3) controls the WAGW (2) with the effect that it exercises policy functionality. Here, however, it is the P-CSCF of the IMS (3) that exercises control of the WAGW (2), instead of a separate P-CSCF in the wireless LAN.

By means of the policy functionality, the P-CSCF of the IMS (3) controls the data traffic through the WAGW (2) and is able to grant, restrict, increase or decline the quantity and quality of the data flow of the MT (6) through the WAGW (2). This mechanism is similar to the one in the Go interface which is installed between the P-CSCF of the IMS (3) and the GGSN of the PS domains. A Go interface is installed between the CSCF (4) of the IMS (3) and the WAGW (2) of the wireless LANs (10) to ensure that data transfer is protected. The WAGW (2) can transmit the SIP messages containing the authentication result via the Gi interface or via the Mm interface to the CSCF (4) in the IMS (3).

Figure 4 shows how the WAGW (2) itself evaluates the authentication result. The WAGW (2) receives the result, which indicates whether an authentication of the MT (6) has taken place in the IMS (3), and the result of this authentication. The WAGW (2) then converts the result by allowing subscriber data to pass through completely or with restrictions. If the WAGW (2) is equipped with a Gi interface, it can transmit authentication messages (SIP registration) via this interface to the CSCF (4) in the IMS (3). Otherwise the Mm interface is used for this purpose. To enable the WAGW (2) to evaluate the result of the authentication (SIP messages), it is implemented in the form of an "application layer gateway". In this way it can convert the result of an SIP authentication accordingly without the assistance of a CSCF (4). The WAGW (2) does this by searching the data packets for SIP messages (registration requests and responses) and interpreting the SIP registration responses accordingly for the filtering of subscriber data. So that the WAGW (2) does not have to open every data packet, a process of elimination is carried out on OSI Layer 3 (IP address) or OSI Layer 4 (port number). Thus an IP address, a port number or other eliminating factor is used to determine whether a data packet or datagram is forwarded to the next higher OSI layer, or whether it may pass through the WAGW (2).

Claims

1. Method for authenticating a subscriber (MT,6) for utilizing services in a wireless LAN (WLAN,10) while using an IP multimedia subsystem (IMS,3) of a mobile radio network,
characterized in that
a subscriber (MT,6) who is to be authenticated and who is located at a location having wireless LAN coverage, receives an IP address from the wireless LAN (WLAN,10) in an attributed manner, after which the subscriber authenticates himself to the IP multimedia subsystem (IMS,3) while giving this IP address, by means of SIP registration, whereby an element (WAGW,2) of the wireless LAN (WLAN,10) is informed of the result of the authentication of the subscriber (MT,6) with regard to the IP multimedia system (IMS,3).

2. Method according to Claim 1,
characterized in that
a subscriber (MT,6) of a wireless LAN (WLAN,10) in an IP multimedia subsystem (IMS,3) is authenticated while using a home subscriber system (HSS,5).

3. Method according to one of the above claims,
characterized in that
a subscriber (MT,6) in a wireless LAN (WLAN,10) in an IP multimedia subsystem (IMS,3) is authenticated while using an authentication server (AAA server).

4. Method according to one of the above claims,
characterized in that

the subscriber (MT,6) transmits, via the wireless LAN (WLAN,10), an SIP register message to a device (CSCF,4) of the IP multimedia system (IMS,3), which transmits a request for authentication of this IP multimedia subsystem (IMS,3) subscriber, using the mechanisms provided for an IP multimedia subsystem authentication, to the home subscriber system (HSS,5), after which the home subscriber system (HSS,5) authenticates the subscriber (MT,6) using these mechanisms and communicates the result of the authentication to the wireless LAN access gateway (WAGW,2).

5. Method according to one of the above claims, characterized in that
an association is implemented between the subscriber terminal (MT,6) and the wireless LAN (WLAN,10) for the purpose of transmitting and receiving via the radio interface between subscriber (MT,6) and wireless LAN (WLAN,10).

6. Method according to one of the above claims, characterized in that
the subscriber terminal (MT,6) receives an IP address from the address area of the wireless LAN (WLAN,10), with which - together with all other IP transport-based data - it can transmit and receive SIP messages that transport authentication messages from and to the IP multimedia subsystem (IMS,3).

7. Method according to one of the above claims, characterized in that

the access to services is controlled via a wireless LAN access gateway (WAGW,2), which monitors successful authentication in the IP multimedia subsystem (IMS,3).

8. Method according to one of the above claims, characterized in that the wireless LAN (WLAN,10) is connected to the IP multimedia subsystem (IMS,3) via a Gi interface.

9. Method according to one of the above claims, characterized in that the wireless LAN (WLAN,10) is connected to the IP multimedia subsystem (IMS,3) via an Mm interface.

10. Method according to one of the above claims, characterized in that the result of the authentication (P-CSCF,1) is fed to the wireless LAN access gateway (WAGW,2) by a (proxy-call state control function)/policy control function (P-CSCF,1) at a location having wireless LAN coverage.

11. Method according to Claim 7, characterized in that the wireless LAN (WLAN,10) has a proxy-call state control function node (P-CSCF,1) which forwards the SIP messages to the corresponding entity in the IP multimedia subsystem (IMS,3) and controls the WLAN access gateway (WAGW,2) with regard to the authentication result of the IP multimedia subsystem (IMS,3).

12. Method according to Claim 7,

characterized in that
instructions are provided to the WLAN access gateway (WAGW,2) on the basis of the result of the authentication in the IP multimedia subsystem (IMS,3), as to how the data traffic of a subscriber (MT,6) is to be handled by the wireless LAN access gateway (WAGW,2), in particular instructions regarding the blocking of data traffic.

13. Method according to one of the above claims,
characterized in that
the proxy-call state control function (P-CSCF,1), by means of a policy control function, controls the data traffic through the wireless LAN access gateway (WAGW,2) and grants, restricts, increases or declines the quantity and/or quality of the data flow of a subscriber (MT,6) through the wireless LAN access gateway (WAGW,2).

14. Method according to one of the above claims,
characterized in that
the policy control function is part of the proxy-call state control function node (P-CSCF,1) or is a separate unit.

15. Method according to one of the above claims,
characterized in that
the result of the authentication is fed to the wireless LAN access gateway (WAGW,2) by the call state control function (CSCF,4) /policy control function in the IP multimedia subsystem (IMS,3).

16. Method according to Claim 12,
characterized in that

the call state control function node (CSCF,4) of the IP multimedia subsystem (IMS,3) controls the wireless LAN access gateway (WAGW,2) with regard to the authentication result of the IP multimedia subsystem (IMS,3).

17. Method according to Claim 13,
characterized in that
a Go interface is installed between the call state control function node (CSCF,4) of the IP multimedia subsystem (IMS,3) and the wireless LAN access gateway (WAGW,2), for protected data transfer.

18. Method according to one of the above claims,
characterized in that
the authentication result is evaluated by expanded functionalities in the wireless LAN access gateway (WAGW,2).

19. Method according to Claim 16,
characterized in that
the authentication result received from the IP multimedia subsystem (IMS,3) is converted by the wireless LAN access gateway (WAGW,2), whereby said WLAN access gateway (WAGW,2) allows subscriber data to pass through completely or with restrictions.

20. Method according to Claim 13,
characterized in that
the evaluation of the authentication result is implemented using an "application layer gateway".

21. Method according to one of the above claims,

characterized in that
the subscriber (MT,6) of the wireless LAN (WLAN,10) is also a subscriber of the mobile communication network.

22. Method according to one of the above claims,
characterized in that
the wireless LAN network (WLAN,10) is integrated into mobile communication networks with the help of ETSI HiperLan and IEEE 802.11.

23. Device for authenticating a subscriber (MT,6) for utilizing services in a wireless LAN (WLAN,10) with the help of an IP multimedia subsystem (IMS,3) of a mobile radio network, said device having

- an IP multimedia system (IMS,3) for authenticating a subscriber (MT,6) who is to be authenticated by means of SIP registration, and who is located at a location having wireless LAN coverage, by giving an IP address allocated by the wireless LAN (WLAN,10), and
- an IP multimedia subsystem (IMS,3) for informing an element (WAGW,2) of the wireless LAN (WLAN,10) of the result of the authentication of the subscriber (MT,6) with regard to the IP multimedia subsystem (IMS,3).

24. Device according to Claim 23,
characterized in that
a device constituting the proxy call state control function node (CSCF,1) is a node in the wireless LAN (WLAN,10).

25. Device according to one of Claims 23 to 24,

characterized in that
the device constituting the proxy call state control function
node (CSCF,1) of the IP multimedia subsystem (IMS,3) is provided for controlling authentication in the wireless LAN (WLAN,10).

26. Device according to one of Claims 23 to 25, characterized in that
the wireless LAN access gateway (WAGW,2) has a device that is configured such that said device converts the authentication result which is received from the IP multimedia subsystem (IMS,3), by allowing subscriber data to pass through completely or with restrictions.